The GDPR and private sector measures to detect criminal activity

Winston Maxwell

The GDPR and private sector measures to detect criminal activity

Winston Maxwell, Director of Law and Digital Technology Studies, Télécom Paris – Institut Polytechnique de Paris

March 2021
(Paper to appear in Law & European Affairs 2021)

Whether it is to fight cybercrime[1], money laundering[2], copyright infringement[3], child pornography[4], the dissemination of terrorist[5] or other forms of illegal content[6], laws increasingly encourage or require private entities to process customer-provided data to detect and/or prevent potentially criminal activity. The delegation of law enforcement functions to private entities raises constitutional issues that we will not examine in this article[7]. Instead, we will focus on the narrower question of how these data processing duties fit with Europe's General Data Protection Regulation (GDPR).[8] We conclude that the delegation of crime-

---

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

[2] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L 141/73 (Fourth AML Directive).

[3] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC OJ L 130/92

[4] Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM/2020/568 final, 10 September 2020.

[5] Position of the Council at first reading with a view of the adoption of a Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, adopted by the Council on 16 March 2021, 14308/1/20 Rev 1

[6] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, 15 December 2020

[7] For an analysis of the U.S. constitutional implications, see Kiel Brennan-Marquez, The Constitutional Limits of Private Surveillance, 66 Kansas L. Rev. 485 (2018), for an analysis of French constitutional implications, see Xavier Latour. La place du secteur privé dans la politique moderne de sécurité. *L'Actualité juridique. Droit administratif*, Dalloz, 2010, pp.657.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (GDPR).

fighting activities to private entities under a risk-based approach conflicts with Articles 10 and 23 of the GDPR, but we offer suggestions for how the problem may be cured.

Traditionally, private entities cooperate with government authorities by responding to specific government or court orders. Laws may require private entities to store particular kinds of data[9] or install technical infrastructure[10] to facilitate subsequent law enforcement requests. Or private entities may act as subcontractors for the government in connection with law enforcement tasks, such as analyzing DNA samples, or providing technological solutions for police surveillance. These forms of passive cooperation raise few issues under the GDPR, at least from the private entity's perspective. The private entity has little or no discretion, and simply follows government instructions; it is not the private entity's job to assess the necessity and proportionality of the government's request.

A new trend is emerging, however, in which legislation defines the objective to achieve, e.g. to detect, prevent and/or report suspected criminal activities, but private entities are asked to determine the best means to achieve the objective based on their own risk analysis. This "risk-based" approach[11] has the advantage of decentralizing decision-making to the entity that has the most information relevant for designing the most appropriate tools to achieve the government's objective. In theory this should lead to more targeted, proportionate, and effective solutions. In practice, the risk-based approach puts the burden on private entities to strike the right balance between interference with privacy and the protection of public security. This displacement of the proportionality analysis conflicts with the philosophy of the GDPR and fundamental rights case law, which require that the necessity and proportionality balance be struck by lawmakers and government, not by private entities. This is why measures that interfere with privacy must be provided for in a law that contains clear and precise rules, including rules that provide adequate safeguards for the rights and

[9] Articles L34-1-1 and R10-13, French Code of Post and Electronic Communications
[10] Article D98-7, French Code of Post and Electronic Communications
[11] Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23 Maastricht Journal of European and Comparative Law 261, at 273, describing the "responsibilization strategy" of co-opting private sector actors to fight crime. In the field of compliance, enlisting the active help of companies to detect and prevent illegal activities by the companies' own employees has long been part of an effective compliance program. This article focuses on the less frequent case in which companies are asked to detect suspicious activity by the companies' customers. On the benefits of a risk-based approach, see Lucia Dalla Pellegrina and Donato Masciandaro, 'The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View' (2009) 5 Review of Law & Economics 931.

freedoms of individuals. The risk-based approach conflicts with a number of specific GDPR provisions, including Article 10 on data relating to criminal offences, and Article 23 relating to restrictions to data subject rights. It also raises questions on the legal basis for processing under Article 6, and on how enterprises should evaluate the necessity and proportionality of their crime-fighting measures in a data protection impact assessment. One of the perverse side effects of risk-based approaches is that companies are incentivized to do too much, rather than too little, to satisfy the law's crime-fighting objectives, a phenomenon known as gold-plating. This poses serious threats for fundamental rights.

The purpose of this article is to confront the risk-based approach with the GDPR and case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). To help focus our analysis, we will concentrate on legislation to fight money laundering and the financing of terrorism (AML/CFT), the draft EU Regulation on fighting of the dissemination of terrorist content, and the draft EU Digital Services Act. The rest of this article is structured as follows: first, we will briefly describe the obligations flowing from AML/CFT legislation and the two draft European regulations referred to above. Second, we will remind readers of the requirements of Article 52(1) of the Charter of Fundamental Rights of the European Union[12] (Charter) and recent case law of the CJEU. Third, we will apply the provisions of the GDPR to the risk-based approaches. Finally, we will make recommendations on how the risk-based approach can be better reconciled with the GDPR and fundamental rights.

1. Three examples of risk-based approaches

Anti-money laundering

The EU's Fourth AML Directive[13] requires banks and other financial institutions to conduct "ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being

[12] Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389 (Charter)

[13] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141/73 (Fourth AML Directive).

conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds".[14] Monitoring must be sufficient to "enable the detection of unusual or suspicious transactions".[15]

Banks and other financial institutions must conduct risk assessments to categorize their business operations and customers into different classes of risks. As a function of the risk classification, customer operations undergo different levels of monitoring based on pre-determined scenarios. The monitoring systems generate alerts when an operation is unusual or suspicious compared to the relevant scenarios. Those alerts are then analyzed by human compliance experts and those experts will in many cases request additional information from the bank customer in order to understand the relevant transaction and gain assurances that it is not linked to illegal activities. If these additional investigations do not clarify the situation, the bank compliance officers will file a report of suspicious activity with the country's financial intelligence unit (FIU), without informing the bank's customer.[16]

The risk-based approach adopted under the Fourth AML Directive puts the responsibility on banks to analyze their own risk profiles and create the automatic monitoring tools that are used to generate alerts. The legal obligation on banks to conduct monitoring is couched in a very general terms. As explained by one commentator, "the Directive shifts the task of investigating financial movements on to the providers of financial services. In such a framework, the providers of financial services serve as an arm of the law enforcement agencies and collaborate in the field of prevention, detection, investigation, and prosecution of crime"[17] Because the sanctions under AML/CFT laws are particularly high, banks have a tendency to err on the side of implementing more monitoring rather than less, and reporting more suspicious activity rather than less.[18] The alerts generated by the automated data processing system of the banks contain a large number of false positives, meaning that many innocent operations are flagged as suspicious.

---

[14] Ibid. art 13(1)(d).

[15] Ibid. art 15(3).

[16] For a more complete description of the monitoring and reporting process, see Astrid Bertrand, Winston Maxwell and Xavier Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights? International Data Privacy Law (2021) (forthcoming).

[17] Jonida Milaj and Carolin Kaiser, 'Retention of data in the new Anti-money Laundering Directive – 'need to know' versus 'nice to know'' (2017) 7 Int'l Data Privacy Law 115, at 118

[18] Michele Sciurba, 'The Incompatibility of Global Anti-Money Laundering Regimes with Human and Civil Rights – Reform Needed?' (Nomos 2019) 9.

After making the decision to send a suspicious activity report to the FIU, the bank often makes the decision to terminate the customer relationship on the grounds that the suspicious activity report creates a suspicion that is incompatible with maintaining the banking relationship. Banks are prohibited from informing customers that they have been the subject of a suspicious activity report. Customers remain in the dark as to why their account was terminated. The large sanctions for violation of anti-money laundering laws also leads banks to conduct so-called de-risking, which consists of terminating banking relationships with groups of customers who are considered high risk by nature. De-risking is controversial because it leads to certain vulnerable groups of the population being targeted, and in some cases being unable to open bank accounts.[19] The AML/CFT systems implemented by financial institutions also rely on watch lists provided by government and private sources.[20] The system will block payments to any person on a list, whether or not the person has actually been convicted of a crime. In sum, the AML/CFT systems implemented by private entities create a serious interference with the right to privacy, but can also lead to discrimination, to violations of the presumption of innocence, and the right to an effective remedy.[21]

Draft Regulation on the Dissemination of Terrorist Content Online

On March 16 2021, the Council of the European Union agreed to a draft regulation on the dissemination of terrorist content online.[22] The draft must now be negotiated with the European Parliament. Recital 3 of the March 16, 2021 draft summarizes the new public-private cooperation approach: "Addressing terrorist content online, which is part of a broader problem of illegal content online, requires a combination of legislative, non-legislative and voluntary measures based on collaboration between authorities and hosting service providers, in a manner that fully respects fundamental rights." Under the proposed regulation, hosting

[19] Ibid., p. 159.
[20] Ibid. p. 73.
[21] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights?, *International Data Privacy Law*, Volume 11, Issue 3, August 2021, Pages 276–293, https://doi.org/10.1093/idpl/ipab010 Michelle Gallant, AML: Maintaining the Balance between Controlling Serious Crime and Human Rights, in Research Handbook on International Financial Crime (Elgar Publishing, 2015); Sara De Vido, Anti-Money Laundering Measures Versus European Fundamental Freedoms and Human rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice, 16 German Law Journal 1271 (2015).
[22] Position of the Council at first reading with a view of the adoption of a Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, adopted by the Council on 16 March 2021, 14308/1/20 Rev 1.

providers become active partners in fighting terrorist content, and are asked to develop a risk-based approach:

"With a view to reducing the accessibility of terrorist content on their services, hosting service providers exposed to terrorist content should put in place specific measures taking into account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information. Hosting service providers should determine what **appropriate, effective and proportionate specific measure should be put in place** to identify and remove terrorist content. Specific measures could include appropriate technical or operational measures or capacities such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content, mechanisms for users to report or flag alleged terrorist content, or any other measures the hosting service provider considers appropriate and effective to address the availability of terrorist content on its services."[23]

The responsibility for determining what measures are "appropriate, effective and proportionate" lies with hosting providers. The sanctions for not implementing those measures can be up to 4% of the hosting provider's global turnover[24].

Draft Digital Services Act

Article 27 of the Commission's proposal for Digital Services Act[25] provides that very large online platforms should perform a risk assessment to identify systemic risks, including systemic risks linked to the dissemination of illegal content. As a function of risks, very large platforms are required to adopt "reasonable, proportionate and effective" mitigation measures "tailored to the specific systemic risks".[26] Most large platforms already use algorithms to identify and remove harmful content on their platforms. These automatic detection and removal tools supplement human flagging under the notice and takedown approach encouraged by the e-Commerce Directive.[27] Platforms already deploy automatic filtering

[23] Ibid, Recital 22 (emphasis added by the author).
[24] Ibid, Article 18(3).
[25] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, 15 December 2020
[26] Ibid, Article 27.
[27] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *OJ L 178/1.*

measures on a voluntary basis to enforce the platforms' terms of use. These measures protect platform users from exposure to 'harmful' content ('harmful' being defined in the platforms' terms of use), and protect the platform's advertising revenues. Advertisers can withdraw their advertising contracts if the platform does not limit the circulation of harmful content. These existing measures protect the platform's business interests. They also happen to contribute to the fight against crime. The Digital Services Act would make a certain level of filtering mandatory for very large platforms, by imposing a new duty to adopt "reasonable, proportionate and effective" measures to fight illegal content as a function of the platform's risk assessment. Platforms would also be obligated to report certain forms of suspicious activity.[28] The sanctions for non-compliance can reach 6% of the platform's annual turnover.[29]

The three examples cited above impose on private entities a duty to implement effective and proportionate measures to detect and in some cases report suspicious illegal activity based on the entities' risk analysis, but without specifying what those effective measures should be. The legislation specifies only that the measures should be proportionate and comply with the GDPR, leaving it to private entities to figure out what this means.

How do these risk-based cooperation mechanisms fare under the GDPR? Before addressing the GDPR, let us summarize the conditions imposed by the Charter.

2. Application of Article 52(1) of the Charter

Article 52(1) of the Charter contains five requirements that must be cumulatively satisfied for a measure restricting fundamental rights to be legal. Under Article 52(1) of the Charter, a measure restricting a fundamental right is lawful if and only if:

1) The measure is provided for by a law that is sufficiently accessible and foreseeable, with clear and precise rules;

2) The measure respects the essence of the fundamental rights at stake;

[28] Ibid Article 21.
[29] Ibid Article 42.

3) The measure is appropriate in that it genuinely meets the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others;

4) The measure is strictly necessary, and in particular it is genuinely effective and the least intrusive available to achieve the objective;

5) The measure is proportionate, and in particular represents a fair balance between the competing rights at stake, and is surrounded by adequate safeguards.[30]

In 2014 and 2016, the CJEU examined data retention obligations imposed on operators of electronic communications. In both the *Digital Rights Ireland*[31] and *Tele2 Sverige - Watson*[32] cases, the CJEU emphasized that a measure interfering with privacy must be provided for by a law with clear and precise rules. The CJEU recognized that the goal of fighting criminality is legitimate and can justify some interference with privacy, but struck down the general obligation to store traffic and location data because the obligation was insufficiently targeted, covering the entire population without distinction. According to the CJEU, there must be some link between the persons whose data are stored and suspicion of a crime. The CJEU found that the processing of traffic and location data could reveal sensitive details about a person's private life, and that the processing therefore created a high level of interference with privacy rights. Indiscriminate and generalized processing of data of all citizens went beyond what was strictly necessary, and did not ensure a fair balance between the competing rights at stake. In the *Tele2 Sverige-Watson* case, the CJEU said that a more targeted approach, requiring retention of data of certain risky groups with links to potential crime, may be permitted, provided there are adequate safeguards including institutional oversight.[33]

[30] The five conditions are presented in detail in European Data Protection Supervisor (EDPS), 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (2017) (EDPS Necessity Toolkit); and EDPS 'Guidelines Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (2019) (EDPS Proportionality Guidelines).
[31] *Digital Rights Ireland v. Minister for Communications*, Joined Cases C-293/12 and C-594/12 [2014] (ECLI:EU:C:2014:238) (Digital Rights Ireland).
[32] *Tele2 Sverige v Post- och telestyrelsen, and Secretary of State v Watson,* Joined Cases C-203/15 and C-698/15 [2016] (ECLI:EU:C:2016:970) (Tele2 Sverige and Watson).
[33] Ibid, para. 111.

In the 2020 *Quadrature du Net*[34] case, the CJEU clarified the scope of Article 4(2) of the Treaty on European Union, holding that national security measures undertaken by the state itself fell outside the scope of EU law, but that measures imposed on private entities remained subject to EU legislation, including the GDPR, even if the objective of the measure was to help fight terrorism. The *Quadrature du Net* case involved a French law permitting intelligence authorities to require operators of electronic communications to analyze communications metadata in real time to detect potential terrorist threats. As in the *Digital Rights Ireland* and *Tele2 Sverige - Watson* cases, the CJEU found that the level of interference with privacy rights was particularly severe, but that serious threats to national security could justify, on a temporary basis, higher levels of interference with privacy. The *Quadrature du Net* decision also considered the legality of using algorithms to analyze data for the purpose of detecting criminal activity. The CJEU identified eight cumulative conditions that must be satisfied in order for such a measure to comply with Article 52(1) of the Charter:

(i) the interference must result from a law containing clear and precise rules;
(ii) a fair balance must be struck between the level of interference with privacy and the seriousness of the crime. A serious threat to national security can justify a higher level of interference than the fight against other forms of crime, including serious crimes;
(iii) institutional review is required by a court or independent regulatory authority to verify respect of all the conditions;
(iv) the algorithm and its results must have a certain degree of transparency and explainability;
(v) the algorithm must satisfy a minimum level of reliability and accuracy in predicting criminal activities;
(vi) the algorithm must be non-discriminatory;
(vii) meaningful human intervention is required to validate or reject the algorithmic recommendation. In the *Quadrature du Net* case, the CJEU said that human review must occur before a decision is taken to launch a more targeted investigation;

[34] *La Quadrature du Net, French Data Network, Order des barreaux francophones et germanophone and others*, Joined Cases C-511/18, C-512/18, and C-520/18 [2020] (ECLI:EU:C:2020:791) (Quadrature du Net).

(viii) the data subject must be notified that he or she has been targeted. Individualized notification can in some cases be delayed to the extent necessary to preserve an ongoing investigation.[35]

Article 52(1) of the Charter deals with laws adopted by the EU and by Member States in application of EU law. What about measures undertaken by private entities in the context of their "risk-based" cooperation with public authorities? Does Article 52(1) of the Charter apply? According to the European Data Protection Supervisor (EDPS), the cooperation of private entities in the fight against criminality must be specified in a law laying down clear and precise rules governing the scope and application of the measure in question.[36] The EDPS refers explicitly to the *Digital Rights Ireland* case[37], stating that the requirement of clear and prices rules should even apply to legislation merely encourages voluntary measures.[38] The risk-based approach does not release the state from the obligation of enacting clear and precise rules. As we will see below, the requirement of clear and precise rules also flows directly from the GDPR.

The same interpretation was given by the European Court of Human Rights (ECtHR) in its decision *Vukota-Bojic v. Switzerland.*[39] The case involved the use of private investigation companies to collect data on persons receiving social insurance benefits in cases where there was a suspicion of fraud. The ECtHR held that states may not absolve themselves from responsibility under the European Convention of Human Rights (ECHR) by delegating its obligations to private bodies or individuals[40]. Consequently the actions of the private entity must have some basis in law and the law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions under which the measures may be undertaken.[41] The law must be particularly precise especially as the technology available is continually becoming more sophisticated.[42] Summarizing ECtHR case law, Ranchorda and

[35] Winston Maxwell, 'La CJUE dessine le noyau dur d'une future régulation des algorithmes', commentaires CJUE 6 octobre 2020, aff. C-511/18 La Quadrature du Net, Légipresse n° 388, décembre 2020, p. 671
[36] European Data Protection Supervisor (EDPS) Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020, p. 8.
[37] Ibid., p. 3.
[38] Ibid, p. 8.

[39] *Vukota-Bojic v. Switzerland*, ECtHR application n° 61838/10, 18 October 2016.
[40] Ibid. para. 47.
[41] Ibid. para. 66.
[42] Ibid. para. 67.

Schuurmans (2019) point out that public authorities "should not evade their obligations by outsourcing tasks to private parties, the standards and underlying values of law enforcement must be the same regardless of whether the enforcement is performed directly by the public authority or a private party with delegated powers".[43]

These decisions confirm that actions taken by a private entity to collaborate with government in the fight against criminality are not exempt from the necessity and proportionality requirements of Article 52(1) of the Charter or Article 8(2) of the ECHR. As we will see below, this conclusion also flows directly from the GDPR.

3. Application of the GDPR to risk-based measures to fight crime

Material scope of the GDPR

The first question relates to the material scope of the GDPR, in particular vis à vis the Police Directive[44], which applies to processing by governmental authorities for the purpose of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties. The GDPR does not apply to data processing that is covered by the Police Directive, but there are two cumulative requirements for the Police Directive to apply: (i) the data controller must be a governmental authority or 'other competent authority', and (ii) the purpose of processing must be prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties. In all other situations, the GDPR applies.[45]

An uncertainty may exist as to whether a private entity processing data for a law-enforcement purpose might be considered an authorized 'competent authority' for purposes of the Police Directive. Article 3(7)(b) of the Police Directive defines competent authority as including "any other body or entity entrusted by Member State law to exercise public authority and

[43] Sofia Ranchordas and Ymre Schuurmans, Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations, University of Groningen Faculty of Law Research Paper Series n° 10/2020, December 2019, p. 37.
[44] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89 (Police Directive).
[45] On the respective scopes of the GDPR and the Police Directive, see Nadezhda Purtova, Between GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships, *International Data Privacy Law*, Volume 8, Issue 1, February 2018, Pages 52–68.

public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". A private entity can in theory become a "competent authority", but it requires a delegation of "public authority and public powers", which means that the private entity must be able to act in the name of the state in certain circumstances. None of the examples of risk-based cooperation noted above confer on the private entity powers to act in the name of the state exercising police powers. These sort of powers might be present in a partial delegation of public powers to private entities, such as the delegation of police powers to security agents of the national railway. But in the case of laws requiring "risk-based" cooperation by private entities, no such delegation exists. Consequently those activities fall solely under the GDPR, not the Police Directive.

Who is data controller?

While the law defines in general terms the purpose of processing, the risk-based approach leaves almost complete discretion to the private entity to determine the means. This leads to the conclusion that the private entity will be considered a separate controller. The European Data Protection Board's (EDPB) guidance on the concept of controller confirms this conclusion, noting that when a law imposes on private entities the obligation to retain or provide certain data to government authorities, the private entities will normally be considered as controllers with respect to the processing that is necessary to execute the obligation imposed by law.[46]

Legal Basis

For risk-based measures to fight criminality, should the legal basis be legitimate interest or compliance with a legal obligation? Or pursuit of a task in the public interest? The Article 29 Working Party has given conflicting signals on this question. In 2011, the Article 29 Working Party said that attempting to rely on legitimate interest or consent as a legal basis for AML/CFT measures would raise "serious difficulties".[47] But the Article 29 Working Party's

---

[46] European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, September 2020, p. 11, para. 22.

[47] Article 29 Working Party, 'Annex to Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing' (WP 186, 13 June 2011), p. 8.

2014 Opinion on legitimate interest says that a data controller may rely on legitimate interest when undertaking voluntary measures to fight crime, even if encouraged by government:

"Finally, the legitimate interest of third parties may also be relevant in a different way. This is the case where a controller - sometimes encouraged by public authorities - is pursuing an interest that corresponds with a general public interest or a third party's interest. This may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as money laundering, child grooming, or illegal file sharing online. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected."[48]

In his 2020 opinion on measures to fight child sexual abuse[49], the EDPS referred to the Article 29 Working Party's 2014 opinion on legitimate interest and confirmed that purely voluntary measures could not be considered as being implemented under a "legal obligation" and that in this case, legitimate interest could be a valid legal basis provided that the three cumulative conditions of the legitimate interest test are satisfied, namely: (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.[50]

Further confusion arises from the EDPS opinion on the draft regulation addressing the dissemination of terrorist content online, where the EDPS mentions "public interest" as a legal basis for voluntary measures.[51] The Fourth AML Directive also mentions "public

[48] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014, p. 28.

[49] EDPS Opinion on the European Commission proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020.

[50] Ibid. para. 21.

[51] European Data Protection Supervisor, Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 10 November 2020, p. 3.

interest"[52] but the EDPS said at the time that legal obligation was the appropriate legal basis, not public interest.[53]

The statements of the Article 29 Working Party and the EDPS are both confusing and contradictory: in 2011, the Article 29 Working Party warned against the practice of "gold-plating" by financial institutions, i.e. going beyond what is strictly required by AML/CFT regulations, and said that relying on legitimate interest would raise "serious difficulties". In 2014, the Article 29 Working Party referred to voluntary measures that go beyond what it legally necessary for AML/CFT, admitting that those voluntary measures could fall under the legitimate interest legal basis. This seems to be an implicit acceptance of voluntary "gold-plating", a practice that the Article 29 Working Party had previously called problematic. The EDPS refers to legitimate interest for purely voluntary measures, but also mentions, in another opinion, public interest. To his credit, the EDPS has consistently complained about the lack of legal certainty flowing from risk-based law enforcement obligations, and has called upon the EU legislators to clearly specify the legal basis of processing in the relevant legislation.[54]

The real debate is not so much between legal obligation and public interest, since both approaches require a basis in law, and the law must contain clear and precise rules which respect the principles of necessity and proportionality. Going down the "legal obligation" path or the "public interest" path leads to the same destination, the requirement of a clear and precise law with appropriate safeguards.

The real debate is whether legitimate interest can be an acceptable legal basis for risk-based law enforcement cooperation measures. The GDPR path for legitimate interest leads in a different direction from the path for legal obligation or public interest, putting the burden on the data controller to assess proportionality through a balancing test. Recitals 47 and 49 of the GDPR state that legitimate interest can justify processing to protect against fraud and against cyberattacks. However, in both those situations, companies are incentivized by their

[52] Article 43, Fourth AML Directive.
[53] European Data Protection Supervisor, Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, 4 July 2013, p. 8.
[54] See most recently, European Data Protection Supervisor (EDPS), 'Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (23 July 2020), p. 11 para. 26.

own business interests to put protective measures in place. They would do so whether or not there existed a legal obligation because it is in their business interest to do so. The same can be said of measures implemented by social media platforms to filter offensive content. These measures help protect advertising revenues, because advertisers would reduce their advertising spending if they feared that their advertisements would be shown in proximity to offensive content. These measures can be said to be truly voluntary because they align with the private entity's business interests. Legitimate interest seems appropriate in these cases. For AML/CFT, however, financial institutions derive no business benefit from monitoring customer transactions and reporting suspicious activity to authorities.[55] Those activities conflict with the traditional duty of bankers, which is to respect banking secrecy. It is highly doubtful that banks would implement such measures in the absence of a legal obligation. Under those circumstances, the measures can hardly be called voluntary, and the only acceptable legal basis would be compliance with a legal obligation, as pointed out in the EDPS's opinion of 2013.[56]

For the draft regulation on terrorist content and the draft Digital Services Act, the question is more complex, because the hosting providers targeted by these laws already undertake a certain amount of monitoring measures in their own interest, but the legislation now creates a legal obligation for them to do so. Should the preexisting measures be covered by legitimate interest and the additional measures be covered by legal obligation? This would create two legal bases applying to different aspects of the same processing, a complexity that is not in the interest of data subjects. There are three reasons to think that once an obligation is imposed by law, the entirety of the processing measures should be based on the "legal obligation" rather than being divided between legitimate interest and legal obligation. The first reason is that applying a single "legal obligation" basis would result in a higher overall protection to data subjects, because that approach would put the responsibility on Member States to define the necessity and proportionality of the measure, as well as define accompanying safeguards in the law. When faced with an ambiguous or incomplete provision, the CJEU prefers an interpretation that furthers the objective that the relevant

[55] Lucia Dalla Pellegrina and Donato Masciandaro, 'The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View' (2009) 5 Review of Law & Economics 931.
[56] European Data Protection Supervisor, Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, 4 July 2013, p. 8.

legislation pursues.[57] In the case of the GDPR, the purpose is to provide a consistent and high level of protection of the rights and freedoms of natural persons with regard to the processing of their personal data.[58] A single legal basis would better achieve this objective. The second reason is that applying a single "legal obligation" basis for the processing also fits better with Article 10 GDPR, which requires that the processing of personal data relating to criminal offenses be authorized by a law providing for appropriate safeguards. Relying on legitimate interest for a portion of the processing and legal obligation for the rest would require showing that the data processed under legitimate interest portion of processing do not relate to criminal offenses, which would seem artificial and difficult. A third reason is that relying on "legal obligation" avoids having to apply a "compatibility" test for further processing under the purpose limitation principle, which we examine now.

Purpose limitation

Under risk-based measures designed to help law enforcement, private entities are generally asked to undertake additional processing operations for data they already have in their possession. The additional processing is for a new purpose, to detect criminal activity, hence we need to ask whether the GDPR's provisions on processing for a secondary purpose apply. The GDPR has a test for determining whether a secondary purpose is compatible with the original purpose.[59] However when processing is based on a legal obligation, Article 6(3) of the GDPR states that the purpose shall be defined in the law. Article 6(4) further states that the data controller need not in that case apply the compatibility test which would normally apply to determine whether the secondary purpose is compatible with the original purpose. If processing were deemed to occur under the legitimate interest legal basis, the data controller would have to show that further processing for the purpose of fighting criminality is compatible with the original purpose. While processing personal data to protect customers against fraud or cyberattacks falls naturally within the sphere of customers' reasonable expectations on the use of his or her data,[60] monitoring actions that can lead to secret reports

[57] Koen Lenaerts and José A. Gutiérrez-Fons To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice 20 Colum. J. Eur. L. 3 (2013-2014)

[58] Recital 10, GDPR.

[59] Article 6(4) GDPR.

[60] Recital 50 GDPR, which refers to the "reasonable expectations of data subjects".

to law enforcement authorities and possible criminal investigations would most likely fall outside of the sphere of the reasonable expectations of customers.

Personal data relating to criminal offenses

A private entity may not process personal data relating to criminal offenses unless authorized to do so by a law that provides for appropriate safeguards for the rights and freedoms of data subjects.[61] To what extent do the risk-based measures involve the processing of personal data relating to criminal offenses? The French Supreme Administrative Court, the *Conseil d'Etat*, considered a system in which a private company, Renault Trucks, analyzed internet traffic of employees to detect possible consultation or exchange of child pornography materials.[62] Renault Trucks argued that the data were not data relating to criminal offenses. The *Conseil d'Etat* did not agree, holding that "personal data relating to criminal offenses" covers not only data related to offenses as such, but also data which are processed with the sole objective of "establishing the existence or preventing the commission of offenses including by third parties".[63] In its opinion in the *Conseil d'Etat* case, the advocate general (*rapporteur public*) said that in order to determine whether the data relate to criminal offenses one must take account of the facts to which the data relate and take a count of the purpose of the processing[64]. The advocate general noted in this case that the processing operations of Renault Trucks transformed the company into an auxiliary of police and judicial authorities, and had the explicit purpose of fighting child pornography.[65] The processing's sole purpose was to detect facts that fall under the classification of criminal offenses. This left little doubt that the data relating to criminal offenses. The UK's ICO adopts a similarly broad definition of data relating to criminal offenses, indicating that the term covers any personal data which are linked to criminal offenses, or which are specifically used to learn something about an individual's criminal record or behavior. According to the ICO, the definition of data relating to criminal offenses also includes suspicions or allegations of criminal activity even though they are not confirmed.[66]

---

[61] Article 10, GDPR.
[62] CE, 11 mai 2015, 375669, *Rec. Lebon*
[63] Ibid, para 6?.
[64] Opinion of Emilie Bokdam-Tognetti, *rapporteur public*,11 May 2015, 375669, p. 4.
[65] Ibid.
[66] Information Commissioner's Office (ICO), What is criminal offence data? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/criminal-offence-data/what-is-criminal-offence-data/ last visited 30 March 2021.

Under these definitions, the processing of data pursuant to a risk-based approach would almost certainly constitute the processing of data relating to criminal offenses, particularly where the processing might lead to a report of suspicious activity to law enforcement authorities. Falling under Article 10 of the GDPR, the processing would therefore require a clear authorization in law with specific safeguards, reinforcing the idea that the only legal basis for processing would be "legal obligation" rather than "legitimate interest". This also raises the question of whether laws imposing risk-based processing are sufficiently clear and precise, a question we will examine below in connection with Article 23 of the GDPR.

Automated decision-making

The next question under the GDPR is whether risk-based systems, which often consist of analyzing customer data to detect suspicious activities, constitute automated decisions under Article 22 of the GDPR. There is no doubt that risk-based systems can result in decisions that produce legal effects or similarly significantly affect individuals. Private companies can terminate customer accounts and even report illegal activities to law enforcement authorities, sometimes without the knowledge of the customer. If the decision is taken by a human after review of the algorithmic recommendation, the processing would not be considered as based solely on automated processing. As pointed out by the Article 29 Working Party, "to qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision."[67]

The existence of meaningful human involvement may also require asking whether human analysts are really making autonomous decisions, or whether they are simply following algorithmic recommendations, a phenomenon known as automation bias[68]. Where analysts must handle thousands of alerts a day, the line between 'meaningful oversight' and 'token gestures' may be difficult to draw.

Regardless of whether Article 22 GDPR applies, algorithmically-generated alerts of illegal content or activities are likely to require human review under the CJEU's *La Quadrature du Net* decision. The CJEU found that one of the required safeguards to accompany invasive

[67] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 as last revised and adopted on 6 February 2018 WP251, p. 21.
[68] Alberdi et al., Why are people's decisions sometimes worse with computer support? Computer Safety, Reliability, and Security Proceedings, 5775, p. 18-31 (2009).

processing is a review of alerts by non-automated means prior to taking any action such as launching targeted surveillance.[69] This conclusion seems directly transposable to monitoring of customer data under risk-based approaches, and is consistent with the Guidelines of the High Level Expert Group (HLEG)[70] and EDPS recommendations.[71]

In some risk-based approaches there is no human involvement at all. Large social media platforms use automated systems that remove many forms of illegal content without any human review.[72] The algorithms escalate to human reviewers cases that are not clear-cut. Content moderation algorithms are accused of creating serious interference with freedom of expression, particularly since they generate a number of false positives, i.e. removals that are not justified[73]. There being no human intervention, Article 22 would likely apply to automatic content removal algorithms[74]. In that case, Article 22 says that the use of such automated means would have to be authorized by law which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, language very similar to that used in Article 10 of the GDPR with respect to data relating to criminal offenses. Article 22 reveals yet another pathway toward the need for a specific law with safeguards. The draft Digital Services Act attempts to provide safeguards for the use of automatic content-removal algorithms, such as an obligation to inform the author of the content, provide reasons for the removal, and a way to contest the decision.

Requirement for a clear and precise law

Here we get to the crux of the problem. Article 23 of the GDPR permits the EU or Member States to restrict rights of data subjects, such as the right to receive information, the right of access personal data, or the right to restrict to processing, "when such a restriction respects

[69] *La Quadrature du Net*, n xx, para 182.
[70] High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, para 64 and 65.
[71] European Data Protection Supervisor, Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 10 November 2020, p. 7.

[72] Cambridge Consultants, Use of AI in Online Content Moderation, Report for OFCOM, 18 July 2019, p. 36.

[73] Winston Maxwell, L'Europe veut encadrer les algorithmes pour retirer les contenus illicites et éviter les « faux positifs », Edition Multimédi@ n° 251, 9 mars 2021, p. 8, see also Gorwa R, Binns R, Katzenbach C. Algorithmic content moderation. Big Data & Society. January 2020.

[74] This assumes that wrongful removal of content creates a legal effect or similarly significant effect for an individual, a question we will not discuss here.

the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard...the prevention, investigation, detection or prosecution of criminal offences." This language follows closely the language of Article 52(1) of the Charter. Recital 19 of the GDPR indicates that restrictions of data subjects' rights exist, for example, in AML/CFT legislation, confirming -- at least for AML/CFT -- that Article 23 applies to such measures. For the draft regulation against the dissemination of terrorist content, Article 23 would also apply because the law provides that in certain cases the data subject must not be informed that terrorist content has been detected, and that data must be stored for six months, both of which are restrictions on data subjects' rights triggering the application of Article 23 GDPR. For the Digital Services Act, the application of Article 23 is more questionable, since the Digital Services Act does not contain the same kind of restrictions of data subject rights as in AML/CFT or in the anti-terrorist content regulation.

Article 23 is important for two reasons.[75] It defines the necessity and proportionality conditions that the law must satisfy when imposing risk-based monitoring, basically repeating the conditions of Article 52(1) of the Charter. Second, Article 23 provides a guideline on the required clarity and precision of the law, listing eight subjects that the law must address: (i) the purposes of the processing; (ii) the categories of personal data, (iii) the scope of the restrictions introduced, (iv) the safeguards to prevent abuse or unlawful access or transfer, (v) the specification of the controller or categories of controllers, (vi)the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing, (vii) the risks to the rights and freedoms of data subjects, (viii) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Article 23(2) makes abundantly clear that the lawmaker, rather than the private entity, should be making the difficult tradeoffs required when balancing privacy rights against the fight against criminality and that the tradeoffs should be addressed explicitly in the law. The legislative provisions that impose risk-based monitoring omit to do this, leaving it to private entities to do the balancing.

---

[75] European Data Protection Board (EDPB), Guidelines 10/2020 on restrictions under Article 23 GDPR, 15 December 2020.

This reveals the major conflict between risk-based approaches and the GDPR. Risk-based approaches have a tendency to outsource the question of necessity and proportionality, including the question of safeguards, to the private sector. The GDPR, and the case law of the CJEU and the ECtHR, require on the contrary that necessity and proportionality be dealt with in the law itself. This is made clear in Recital 41 of the GDPR, which states that the "legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the Court of Justice) and the European Court of Human Rights." When considering a proposal relating to the "voluntary" detection, removal and reporting of child sexual abuse online, the EDPS emphasized that given the nature of the interference, the proposed measures must be accompanied by a comprehensive legal framework, with clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards.[76]

Article 23 simply repeats and specifies conditions that already exist in Article 52(1) of the Charter and the case law of the CJEU. The CJEU case law has held that monitoring practices to detect potential criminal activity create serious interferences with privacy, but those interferences can be justified if the conditions of Article 52(1) of the Charter are satisfied. One of those conditions is the existence of a law that contains clear and precise rules. We have seen that several articles of the GDPR call for a law providing for appropriate safeguards for the rights and freedoms of data subjects. Recital 41 reminds us that the law must be clear and precise. And yet clarity and precision are lacking from the laws imposing risk-based approaches.

Data protection impact assessments

The last GDPR provision involved in risk-based measures to fight crime is Article 35, which requires data protection impact assessments for high risk processing. Article 35 of the GDPR requires data controllers to prepare a data protection impact assessment for any high risk processing. The definition of high risk processing includes any large scale processing operations which are likely to result in a high risk for example on account of their sensitivity and which result in a high risk to the rights and freedoms of data subjects.[77] The processing of

[76] European Data Protection Supervisor (EDPS) Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020, p. 8.
[77] Recital 91 GDPR.

data related to criminal offences is given as an example. Monitoring of customer data to detect illegal activities will almost certainly be considered high risk processing, resulting in the need to prepare a data protection impact assessment. The data production impact assessment requires among other things an assessment of the necessity and proportionality of the processing operations in relation to the purposes.[78] For risk-based monitoring measures imposed by law, how is the private entity to judge their necessity and proportionality? Is the question of proportionality simply whether the risk-based measures implemented by the company go beyond what is legally required? Or is the question broader, whether the risk-based measures are necessary and proportionate in relation to the objective of fighting crime fixed by the law?

The data protection impact assessment might limit itself to risks that are solely within the control of the private entity, such as security risks. The purpose of the impact assessment would then focus solely on technical measures to mitigate those security risks. But the risk-based approach also asks the private entity to decide what data it should be examining, for which customers, and using what technology. It seems unfair to put the burden on private entities to determine the necessity and proportionality of using certain types of data processing techniques (AI?) to identify criminal activity, particularly since one of the requirements imposed by law is that the techniques be "effective". As has been noted in connection with AML/CFT, the lack of specifications in the law, and the threat of sanctions, can lead private sector entities to err on the side of over-monitoring.

4. Recommendations to reconcile risk-based approaches and the GDPR

Enlisting the help of private actors to fight crime under a risk based approach makes sense. Private actors are in many cases the best or only source of data that can lead to the detection and prevention of crime. Private actors are also in the best position to develop approaches that are proportionate, focusing on the most serious crimes and the most risky portions of their customer base. This is fully consistent with the CJEU's approach in the *Digital Rights Ireland* and *Tele2 Sverige – Watson* cases, which says that data retention obligations should be targeted. A top-down, one-size-fits all, approach dictated by the government would likely prove less effective and more intrusive than a risk-based approach developed by the private

[78] Article 35(7) GDPR.

entity that is closest to the data and the persons being monitored.

However the risk-based approach conflicts with the philosophy of the GDPR and fundamental rights case law. According to this philosophy, the legislature should strike the appropriate balance between the objective of fighting criminality and the interference with individual rights, and this balance should be materialized in a law laying down clear and precise rules governing the scope and application of the measure in question.[79] Private actors should not be asked to strike this balance in the place of public authorities. Ideally, the involvement of private actors should be defined with precision in a law addressing all the issues listed in Article 23(2) of the GDPR.

Is the risk-based approach irreconcilable with the GDPR? The draft regulation on the dissemination of terrorist content on line provides for safeguards for the rights of the providers of content. The regulation also provides for a duration for the storage of data. The same is true for the draft Digital Services Act, which requires that algorithmic removals be notified to the providers of the content and that reasons be given for the removal. These texts do not contain all the details specified in Article 23(2) of the GDPR, but they address some of the questions of adequate safeguards.

The major gap that remains is that private actors are basically alone in defining what data processing measures are effective and proportionate to achieve the objectives defined by the law. Article 35 requires preparation of a data impact assessment and analysis of necessity and proportionality, but the scope of what the company is supposed to assess is unclear. Article 36 of the GDPR requires consultation of the data protection authority (DPA) whenever a data protection impact assessment shows the existence of high risks even after application of mitigation measures.[80] However Article 36 is rarely applied in practice because consulting the DPA under Article 36 amounts to an admission that mitigation measures proposed by the

[79] *Digital Rights Ireland*, para. 54.

[80] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to results in a high risk" for purposes of Regulation 2016/679, 4 April 2017 as last revised and adopted on 4 October 2017, WP 248, p. 18-19.

company are not sufficient, and that the data processing operation is disproportionate and therefore illegal.

One possible way to help close the gap between the risk-based approach and the philosophy of the GDPR would be to require consultation of the DPA under Article 36 whenever the data processing involves data related to criminal offenses. The private company would be obligated to prepare data protection impact assessment under Article 35 and propose mitigation measures. However, the company would not be alone in determining the right balance between protecting the rights and freedoms of individuals and achieving the anti-crime objective imposed by law. The details of the company's impact assessment and the consultations with the DPA may have to remain confidential since they may reveal the techniques used by the company to detect criminal activity. Disclosing those techniques would permit criminals to avoid them. If recourse is made to Article 36 of the GDPR, individual measures adopted by companies would be subject to review by the country's data protection authority to help ensure that the measures are strictly necessary to comply with the requirements of the law. Such an approach would breathe new life into Article 36 of the GPPR, as well as helping close the gap that currently exists between risk-based measures and requirements of the GDPR. This approach would amount to adopting to an authorization regime for processing of data relating to criminal offenses, and approach that existed in France before adoption of the GDPR. It is consistent with the intent of Article 36(5) of the GDPR, which permits Member States to make DPA consultation obligatory when processing is done for the performance of a task in the public interest.

Another step to close the gap would be for the law imposing anti-crime measures to provide general guidelines on the measures that should be implemented by private entities, and authorize the government to define by decree more precise technical measures applicable to different actors in the industry, covering the key issues mentioned in Article 23(2) of the GDPR. Individual measures taken by each company could even be covered in a confidential government ruling, an approach used in French cyber-security regulations applicable to companies operating infrastructure of vital importance.[81] This approach would permit the proportionality balance to be made in the first instance in the law itself, at a second level by

[81] Article R1332-41-1 of the French Defense Code, which provides that details of cybersecurity rules for a particular installation of vital importance may be issued in a confidential ruling.

the government in a decree, and at a third level by individual companies in cooperation with public authorities when they define the precise measures to be implemented at a company level – a form of co-regulation. Each of these measures would be subject to review by courts to determine their proportionality in accordance with Article 52(1) of the Charter.

It is the role of public authorities, not private entities, to define and impose duties relating to the public interest. Risk-based approaches tend to mix up the roles of private actors and public authorities by giving discretion to private actors to define appropriate measures to attain public interest objectives. While this approach has benefits, it also carries risks for fundamental rights. In the field of fighting criminality, choosing the appropriate level of technical measures often boils down to balancing interference with citizens' privacy rights against protection of public security, a balancing that should be done by legislatures and governments. We do not advocate abandoning risk-based approaches, but instead emphasize the need for greater specification in legal texts, and greater oversight by regulatory authorities to ensure that measures adopted by companies under risk-based approaches respect the principles of Article 52(1) of the Charter.